MATH 495R, HOMEWORK 11
RSA CRYPTOGRAPHY

In this lab we will implement the RSA public key cryptosystem.

Recall that for any number N, and any a relatively prime to N, we have that

$$a^{\phi(N)} \equiv 1 \pmod{N}.$$

Hence, if $k \equiv 1 \pmod{\phi(N)}$, we can write $k = 1 + \ell\phi(N)$, and we have

$$a^k = a^1(a^{\phi(N)})^\ell \equiv a \pmod{N}.$$

In order to create an RSA key pair, we will find an integer N that is a product of two large primes p and q. For this value of N, we know that $\phi(N) = (p-1)(q-1)$. We will choose an e that is relatively prime to $\phi(N)$ (usually the prime 1234577 will work). Then we compute d such that $de \equiv 1 \pmod{\Phi(N)}$. The public key is the pair

$$[e, N]$$

and the private key (which must be kept secret) is the pair

$$[d, N].$$

To encrypt a message to a person, you first look up their public key $[e, N]$. Convert your message to a number M using the 100 character alphabet (from last semester). Then compute

$$C \equiv M^e \pmod{N} \qquad \text{with } 0 \leq C < N.$$

This number is the encrypted message that is sent.

To decrypt a message C sent to you that is encrypted as above with your public key $[e, N]$, you would compute

$$P \equiv C^d \pmod{N} \qquad \text{with } 0 \leq P < N.$$

Since $C \equiv M^e \pmod{N}$, we see that $P \equiv (M^e)^d \equiv M^{de} \equiv M \pmod{N}$, since $de \equiv 1 \pmod{\phi(N)}$. Hence, you would retrieve the original message. Note that you should be the only one who knows your private key, so you should be the only one able to read the message.

If two people, Alice and Bob, each have a public/private key pair (say Alice's is $[e_A, N_A]$ and $[d_A, N_A]$ and Bob's is $[e_B, N_B]$ and $[d_B, N_B]$), then Alice can send Bob an encrypted and signed message as follows.

Let M be a number smaller than N representing the message. Then Alice encrypts it using Bob's public key $[e_B, N_B]$ to get

$$C \equiv M^{e_B} \pmod{N_B} \qquad \text{with } 0 \leq C < N_B.$$

Alice will then take the encrypted text C and run it though her decryption key (which is something that only she can do) to get a signature:

$$S \equiv C^{d_A} \pmod{N_A} \qquad \text{with } 0 \leq S < N_A.$$

She then sends Bob the pair of numbers (C, S). Using his decryption key (which only he can do), Bob can decrypt C to obtain and read M. Using Alice's encryption key (which is publicly known) on S will result in a number $V \equiv S^{e_A} \pmod{N_A}$. If $V \equiv C \pmod{N_A}$, this verifies that the message comes from Alice. If $V \not\equiv C \pmod{N_A}$, then the message is not from Alice.

Your assignment:

1. Create three functions:
   (a) A function `createkey(p,q)` that takes two large primes `p` and `q`, and creates a public key $[e, N]$ and a private key $[d, N]$ where $N = pq$ and e is the smallest number larger that 1234576 that is relatively prime to $\phi(N) = (p-1)(q-1)$.
   (b) A function `encrypt(message,EKey)` that takes a string and a public encryption key, and returns an integer C that is the RSA encrypted message.
   (c) A function `decrypt(C,DKey)` that takes an integer and a private decryption key, and returns the decrypted message as a string.
2. A list of large primes (over 100 digits) has been placed online at

   `http://math.byu.edu/~doud/RSA/largeprimes`

   Using the first two primes from this list, create a public/private key pair. Encrypt the message "I have finished part 2 of the assignment!" using the public key. You should probably check that the private key, together with your `decrypt` function, correctly decrypts the message.
3. You have an RSA key contained in the web page:

   `http://math.byu.edu/~doud/RSA/keypair`

   Note that this page contains both a public (encryption) key, EKEY, and an private (decryption) key, DKEY. It also contains a number C, which is an encrypted message that has been sent to you, encrypted with EKEY.

   Decrypt the message!
4. A message has been encrypted using a key created in exactly the way specified in problem two; by choosing two primes from the list of large primes, and creating a key. The public key used (and the number C representing the encrypted message) can be found in the webpage

   `http://math.byu.edu/~doud/RSA/publickey`

   Find the private (decryption) key and decrypt the message!
5. Write a function `verifysignature(C,S,EKey)` which takes as input an encrypted message C, a signature S, and the encryption key of the purported sender. Both C and S will be integers. The function should return True if the signature is valid, and False otherwise.

   As before, your RSA key is found at

   `http://math.byu.edu/~doud/RSA/keypair`

   Two people, each claiming to be Alice, have sent you a message encrypted with your public key. Both messages (and their signatures) are contained in the web page

   `http://math.byu.edu/~doud/RSA/SignedMessages`

   Assuming that Alice keeps her private key secret, and using the list of public keys at

   `http://math.byu.edu/~doud/RSA/PublicKeyDatabase`

   decrypt both messages and check the signatures to determine which (if any) of the two messages is really from Alice. Can you tell who the other one is from?